CyOTE CASE STUDY: CRASHOVERRIDE/INDUSTROYER

NOVEMBER 18, 2021

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL Idaho National Laboratory

Table of Contents

CYOTE CASE STUDY: CRASHOVERRIDE/INDUSTROYER

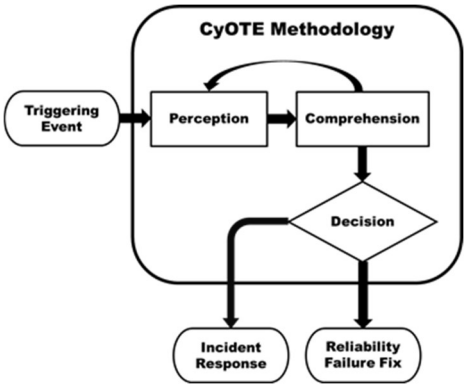
INTRODUCTION

The CyOTE methodology developed capabilities for energy sector asset owners and operators (AOOs) to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE), CyOTE is a partnership with energy sector owners and operators. CyOTE seeks to tie effects of a cyber-attack to anomalies—as detected by commercial or in-house solutions—in the OT environment to determine if it has a malicious cyber cause.

Case Studies support continued learning through analysis of incidents and events. Some of the richest and most detailed Case Studies are expected to be produced by AOOs who have employed the CyOTE methodology to perceive and comprehend actual triggering events in their OT environments, with the benefit of complete access to all data and full context. To bootstrap the learning process and complement anticipated AOO-generated Case Studies, the CyOTE team has begun compiling Case Studies of historical OT attacks and OT-related incidents.

This historical Case Study is based on publicly available reports of the incident from media outlets and cybersecurity firms instead of the full context and data that an AOO would have. This Case Study is not, nor is it intended to be, completely comparable in detail or structure, nonetheless it provides examples of how key concepts in the CyOTE methodology look in the real world. Perhaps more importantly, evaluating this historical incident through the CyOTE methodology provides a learning opportunity from the perspective of "how could this have been detected?" instead of "why was this missed?" to grow the body of knowledge on perception, comprehension, and organizational capabilities.

METHODOLOGY



The CyOTE methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. MITRE's ATT&CK® Framework for Industrial Control Systems (ICS)[1] is used as a common lexicon to assess triggering events related to three Use Cases – Alarm Logs, Human-Machine Interface (HMI), and Remote Logins – which together account for 87 percent of the techniques commonly used by adversaries. The CyOTE methodology is also appropriate for OT-related anomalies perceived outside the three Use Cases, such as through the energy system itself.

The Case Study highlights the CyOTE methodology for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation – a triggering event – is perceived, and continues to the point where the anomaly is comprehended with sufficient

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

confidence to make a business risk decision on the appropriate resolution. If sufficient evidence of a malicious nexus is found, then the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to the situation addressed through existing organizational corrective maintenance and work management procedures.

By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. CyOTE can assist AOOs in prioritizing their OT environment visibility investments. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

BACKGROUND ON THE ATTACK

In December 2016, malware was activated within Ukrenergo, a Ukrainian power grid company, causing a single substation to open all circuit breakers by utilizing the Remote Terminal Units (RTUs). This created a blackout within Ukraine's capital, Kiev, leaving 225,000 people without power for six hours during the dangerous temperatures of winter.

Shortly after the incident, the Slovakian anti-virus firm, called ESET, was tasked with investigating the malware, initially referred to as "Industroyer" due to its targeting of industrial control processes. ESET consulted with Dragos in June 2017, and the malware name was changed to "CRASHOVERRIDE" due to numerous indicators within the code labeled "Crash." Evidence gathered in Dragos's findings suggested the malware first prevented operators from monitoring specific systems. Later, it exploited a known vulnerability that sends an electrical charge to the Siemens SIPROTEC protective relay, causing it to shut off.

MAP OF ATTACK TTPS

By mapping the techniques, tactics, and procedures an attacker used to gain access, CyOTE researchers examined where greater monitoring and detection could provide the visibility needed to connect the dots on attacker activity. The CRASHOVERRIDE incident involved the use of adversary techniques from all three CyOTE Use Cases – Alarm Logs, HMI, and Remote Logins. Twenty-five techniques were identified as part of this complex attack campaign. Figure 1 demonstrates pivot points used by the adversary and does not indicate linear use of techniques within a given timeline. AOOs can utilize this information in their own environments to quickly identify potential attacks and take mitigative actions.

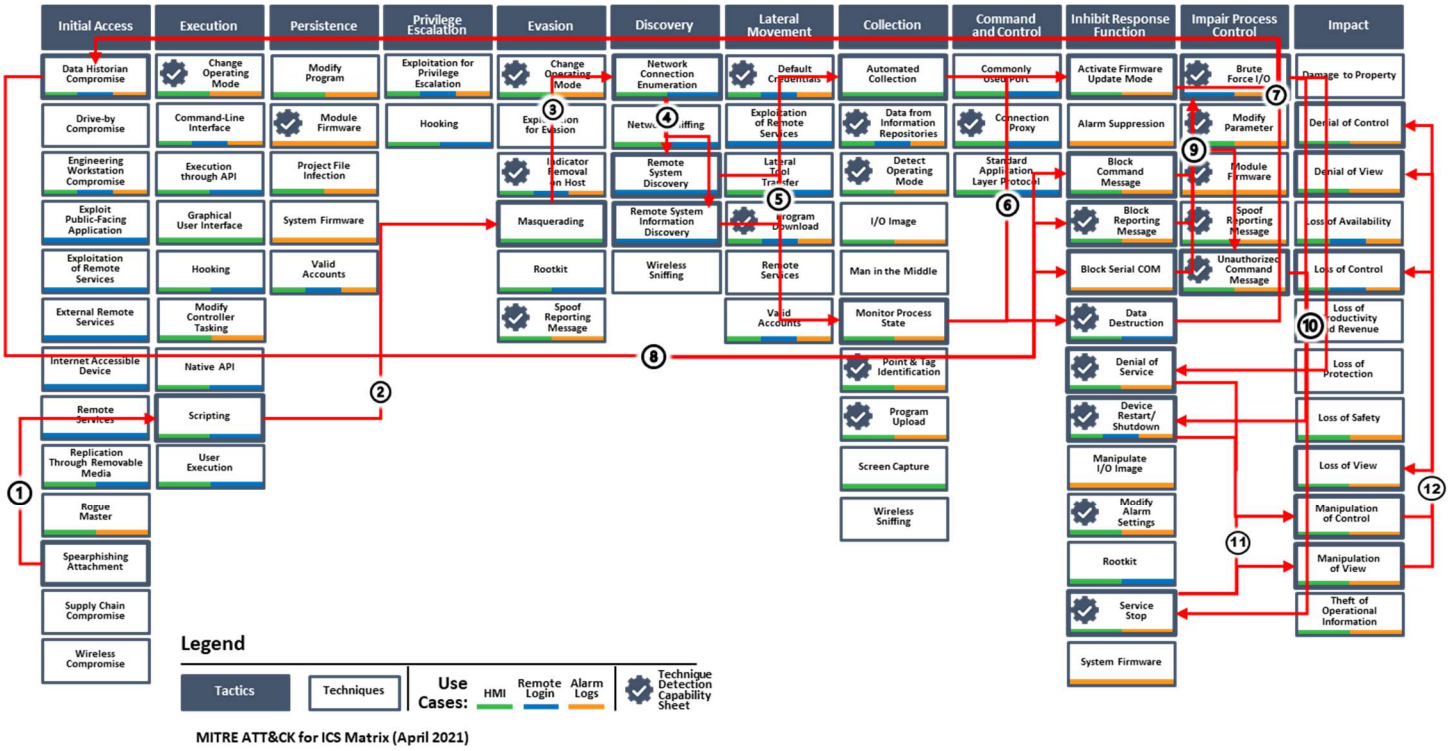


Figure 1. CRASHOVERRIDE/Industroyer Incident Adversary Techniques Chain

APPLICATION OF CyOTE METHODOLOGY AND TECHNIQUES TO THE ATTACK PATH

Anomalies, possible related adversary techniques, and example perception methods for the anomalies, broken down by general adversary campaign steps, are detailed below.

The chart shown in Figure 2 clearly lays out the multiple techniques implemented at the time. From initial access to network connection enumeration, the adversary was able to silently monitor and gain knowledge of the system they had infected. Although there is no confirmed consensus on when and how the adversary gained initial access, researchers agree that the start of the impact phase was the Data Historian compromise. Once adversaries gained access to the Data Historian and initiated the compromise technique, they were able to cause impactful and damaging changes, including blocking command messages, restarting equipment, and reaching their end goal—manipulation and control of industrial processes. By the time operators had lost control of their substation, the impact state was already in full effect.[2]

[2] https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Slowik.pdf

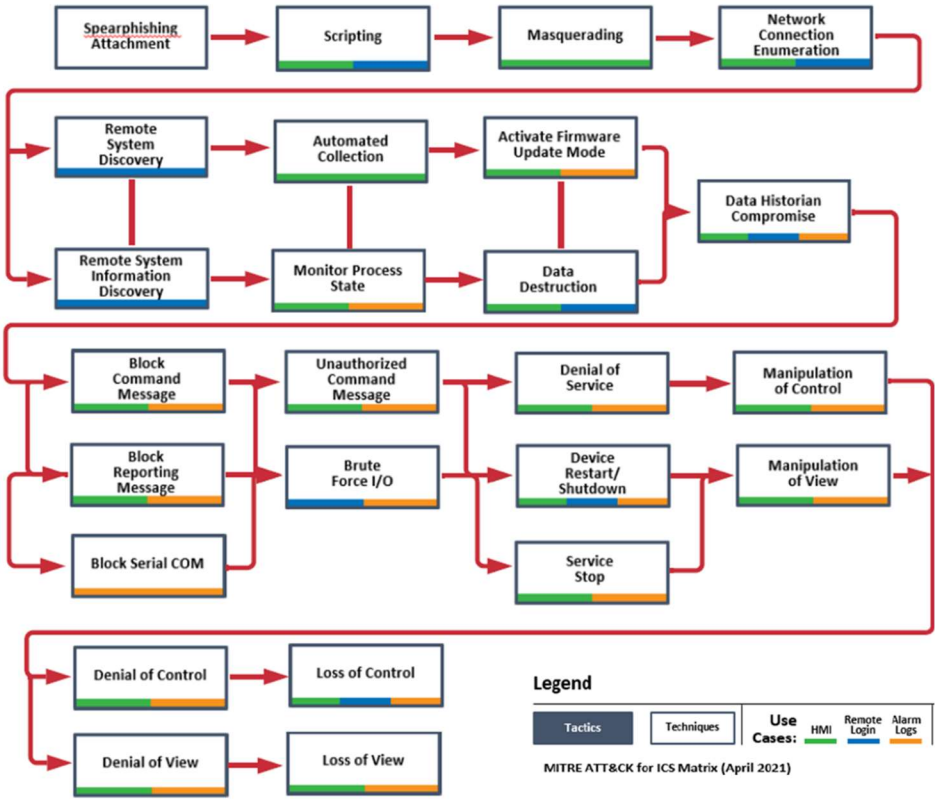


Figure 2. CRASHOVERRIDE/Industroyer Attack Path

The key to identifying this attack prior to impact is to think about where a monitoring tool could be placed earliest in the cyber-attack kill chain. Several techniques may have been comprehended earlier, had relevant data sources been identified:

- T846 Remote System Discovery – As an adversary is attempting to assemble the missing pieces and gain a better picture of the network they are in, this discovery system leaves logs within the control process which, when monitored, would alert of suspicious activity.
- T800 Activate Firmware Update Mode has 26 data sources that provide different angles of perception for any AOO, thereby increasing defensive capabilities.[3]

Event Perception

A number of anomalies could have been recognized through monitoring which, when considered together, could have been identified as a triggering event. The following were identified externally as indicators of compromise:

- Increase of packet traffic
    - Operators would have been able to observe an increase in network traffic, potentially coming from a malicious IP address
- Blocking of command messages
- Scanning of IT and OT network with a variety of protocols (relates to Alarm Logs Use Case)
    - Would generate abnormal log entries

[3] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

- Remote Desktop Protocol sessions initiated without authorization (relates to Remote Login Use Case)
- Equipment restart

Had the last two anomalies listed been observed and comprehended, a triggering event could have been declared prior to the impact phase of the cyber-attack. Network Protocol Analysis and Packet Capture have been identified as viable data sources to monitor for anomalies. Out of 63 reported techniques, Network Protocol Analysis appears in 33 techniques as a viable data source and Packet Capture likewise appears in 36.

Event Comprehension

Additional anomalous behavior could have been identified leading to detection of a cyber-attack:

- Traversal across the network (relates to Remote Login Use Case)
- Known executable running in a different location (related to HMI Use Case)
- Firmware updates to SIPROTEC relays (relates to Alarm Logs Use Case)
- File Monitoring of ICS configuration files

Additionally, physical anomalies could have been detected, had they occurred in a different stage of attack. Firmware Update Mode occurred at the impact stage of the cyber-attack kill chain in this case study, limiting response time. While Stuxnet's replacement of PLC firmware was an observable that occurred, it would have remained dormant, executing the replaced firmware directives. Across a greater period of time, this observable would prove integral to mitigation if not dismissed as a mechanical failure. Here, an operator could have perceived several previous disruption events:

- Increase in Phishing campaign, starting as early as January 2016, could have been perceived through a properly configured firewall giving alerts to an unusually high number of attempts.
- SIPROTEC Relays mis-operating or failing to perform their designated functions would have increased substation downtime prior to impact, and potentially resulted in a higher amount of required technician visits to repair and replace parts. Had this data been monitored, it could have alerted an AOO to nefarious activity within a system.
- Multiple RTUs going down or having the same cyber-enabled Firmware Update Mode activated without command from proper channels. Had this data been monitored, it could have alerted an AOO to nefarious activity within a system.[4]

Event Decision

Building upon the perception and comprehension of anomalies leading to triggering events requiring rapid response, decisions must be made. Operators observing an unusual amount of PLCs being activated into firmware update mode or noticing an abnormal number of "disruption events" signal suspicious behavior. By reporting anomalies through the correct channels, an AOO could quickly identify triggering events, build comprehension, and make a better risk-informed decision to respond to a security event earlier in the attack chain.

[4] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

CONCLUSION

The CRASHOVERRIDE Case Study emphasizes how the CyOTE methodology can be utilized by AOOs, even at different maturity levels, to identify cyber attack techniques within operational technology environments earlier along a complex attack chain. Using the CyOTE methodology, an AOO can filter signal from noise to identify interconnected anomalies, trigger further investigation, and escalate response procedures. AOOs can utilize commercial tools and/or CyOTE capabilities to increase visibility and comprehension across the three CyOTE Use Cases. Deeper comprehension will allow AOOs to successfully identify and comprehend indicators of attack earlier in the campaign in order to respond to and resolve incidents with ever decreasing impacts. Furthermore, deeper comprehension of the OT environment provides AOOs sufficient confidence to make risk-informed decisions on whether or not to declare a cybersecurity incident and begin response procedures in the OT environment when anomalies occur outside the OT environment.

SCENARIO CONSIDERATIONS

After reviewing this Case Study, AOOs should consider how a similar scenario could unfold in their operating environment, determine the level and location of visibility necessary for them to perceive the triggering event and other anomalies, and identify accessible information sources to build comprehension. The following questions for reflection and discussion can help AOOs prepare to employ the CyOTE Methodology in their organization.

- Could you perceive a similar triggering event in your organization? How would it be perceived, and by whom?
- What anomalies exist that could have been perceived earlier than the triggering event was? How would each be perceived, and by whom?
- Who will you contact from the System Operations, Engineering, and Cybersecurity departments to build comprehension? Would they be willing and able to assist today?
- How much evidence would you need to confidently reject the null hypothesis of a reliability failure, and initiate cybersecurity incident response procedures?
- Who else in your organization needs to be aware of the outcome?

AOOs can refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557